

Docket No. RSW920030303US1

**METHOD AND APPARATUS FOR ALTERNATIVE REGISTRY LOOKUP OF  
WEB SERVICES**

**BACKGROUND OF THE INVENTION**

5

**1. Technical Field:**

The present invention relates generally to Web services architecture. In particular, the present invention provides a method and apparatus for registry 10 lookup of Web services. Still more particularly, the present invention provides a method and apparatus for alternative registry lookup of Web services without impacting existing client implementation.

15 **2. Description of Related Art:**

In recent years, the use of Internet has greatly increased as more consumers are connecting to the World Wide Web. As a result, consumers demand a wider variety of services to be available online. In order to meet 20 this demand, vendors make their services available by using a mechanism called Web services.

Generally, Web services are services offered by one application, such as a vendor Web site, to other applications, such as consumer applications, via the 25 World Wide Web. By obtaining Web services, consumer or client applications may aggregate these services to enable business transactions. An example Web service may be a client requesting a stock quote online, in which the request of the current price for a specific stock is sent 30 from the client application to a service provider. This

Docket No. RSW920030303US1

request is sent to a given universal resource locator (URL) using common networking communication protocols, such as, for example, simple object access protocol (SOAP) and hypertext transfer protocol (HTTP). The URL 5 identifies the location of the service provider or the service endpoint location. When the service provider receives and processes the request, a response is sent from the service provider using similar protocols to the client application. In this example, the stock price for 10 the requested stock is returned to the client application.

In order to make their services available for client applications, service providers define abstract service descriptions using a language called Web Services 15 Description Language (WSDL), a language specification available from the World Wide Web Consortium (W3C). WSDL provides definition of a service endpoint in the form of a markup language. A concrete service, known as the concrete service description, is created using the 20 abstract service description in WSDL. Service providers may then publish the concrete service description to a registry, such as, for example, a universal description, discovery and integration (UDDI). Using a registry mechanism like UDDI, a service requestor locates a 25 service description from which the requestor selects and uses a concrete implementation of the service.

Currently, existing client applications locate service providers in a registry dynamically. Even when a URL of the service provider changes, in failover 30 situations, or multiple implementations of WSDL port type

Docket No. RSW920030303US1

exist for a client to potentially use, a client application may still locate the service provider, but only if custom coding for dynamic lookup is incorporated into the client application explicitly. No standardized mechanism specifying where and how to look up an endpoint location for a Web service currently exists.

Existing lookup mechanisms, such as, for example, Java API for XML registries (JAXR) and UDDI for Java (UDDI4J), require developers of client applications to perform registry lookup each time a service is requested. This repetitive lookup uses machine resources for each lookup and adds to the client execution time as additional requests are sent from the client application. In addition, changes to existing client application implementation are required when location of the service endpoint changes.

Furthermore, existing lookup and registry mechanisms conflict with other solutions, such as, for example, Java API for XML-based remote procedure call (JAX-RPC) and Web services for Java 2 enterprise editor (JSR-109), products available from Sun Microsystems, Inc. These mechanisms use a naming and directory technology called Java naming and directory interface (JNDI) application programming interface (API), which provides methods for client applications to access Web services.

Therefore, it would be advantageous to have an improved method, apparatus and computer instructions for alternative registry lookup of Web services without impacting existing client implementation. It would also

Docket No. RSW920030303US1

be advantageous to have an improved method that leverages existing standards like JAX-RPC and J2EE Web services.

Docket No. RSW920030303US1

#### SUMMARY OF THE INVENTION

The present invention provides a method, apparatus, and computer instructions in a data processing system for alternative registry lookup of Web services without impacting existing client implementations. A client application container is provided with an alternative registry lookup Java naming and directory interface (JNDI) provider for accessing Web services. When a client application or service requester requests a Web service, instead of using a Web service description language file directly to locate the service endpoint, the alternative registry lookup JNDI provider is used to determine if a service-ref-name element corresponding to requested service name is present in a new registry file by examining the file.

If the service-ref-name element is present, the alternative registry lookup JNDI provider identifies the service endpoint URL for the requested service name using information from the new registry file to perform lookup in the registry. However, if the service-ref-name element is not present in the new registry file, the alternative registry JNDI lookup provider defers the lookup operation to a standard JNDI provider. The standard JNDI provider then searches a webservicesclient.xml file with the service-ref-name element and locates a WSDL file corresponding to the service-ref-name element by examining the wsdl-file element of the webservicesclient.xml file.

Once the WSDL file is located, the standard JNDI provider determines if the requested service name of the

Docket No. RSW920030303US1

service-ref-name element maps to the wsdl:service element of the WSDL file. If a mapping occurs, the service endpoint URL is identified from the wsdlsoap:address element of the WSDL file.

5        In addition, the alternative registry lookup JNDI provider may implement a lookup policy in the new registry file in the event of multiple service endpoint URLs so that only a single service endpoint URL is returned to the service requester.

Docket No. RSW920030303US1

**BRIEF DESCRIPTION OF THE DRAWINGS**

The novel features believed characteristic of the invention are set forth in the appended claims. The 5 invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

10       **Figure 1** is a pictorial representation of a network of data processing systems in which the present invention may be implemented;

15       **Figure 2** is a block diagram of a data processing system that may be implemented as a server in accordance with a preferred embodiment of the present invention;

**Figure 3** is a block diagram illustrating a data processing system in which the present invention may be implemented;

20       **Figure 4A** is a diagram illustrating relationships between JNDI providers of the present invention in accordance with a preferred embodiment of the present invention;

25       **Figure 4B** is a diagram illustrating an example implementation of delegating lookup to a standard JNDI provider in accordance with the present invention;

**Figure 5** is a diagram of components used in the present invention in a preferred embodiment of the present invention;

Docket No. RSW920030303US1

**Figure 6** is a diagram illustrating interaction between components used in the present invention in a preferred embodiment of the present invention;

5       **Figure 7** is a diagram illustrating an example client container implementation in accordance with a preferred embodiment of the present invention;

10      **Figure 8** is a diagram illustrating an example implementation of the webservicesclient.xml file in accordance with a preferred embodiment of the present invention;

**Figure 9** is a diagram illustrating an example implementation of a WSDL file in accordance of the present invention;

15      **Figure 10** is a flowchart diagram illustrating an exemplary process of performing alternative registry lookup in accordance with a preferred embodiment of the present invention;

20      **Figure 11** is a flowchart diagram illustrating an exemplary process of registry lookup performed by a standard JNDI provider in accordance with a preferred embodiment of the present invention;

**Figure 12** is a diagram illustrating an example implementation of a UDDI registry provider in accordance with a preferred embodiment of the present invention;

25      **Figure 13** is a diagram illustrating an example implementation of the UDDI registry file using a keyed policy in accordance with a preferred embodiment of the present invention; and

**Figure 14** is a diagram illustrating an example UDDI registry file using a lookup policy of the present

Docket No. RSW920030303US1

invention in accordance with a preferred embodiment of  
the present invention.

Docket No. RSW920030303US1

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT**

With reference now to the figures, **Figure 1** depicts a pictorial representation of a network of data processing systems in which the present invention may be implemented.

5 Network data processing system **100** is a network of computers in which the present invention may be implemented. Network data processing system **100** contains a network **102**, which is the medium used to provide communication links between various devices and computers  
10 connected together within network data processing system **100**. Network **102** may include connections, such as wire, wireless communication links, or fiber optic cables.

In the depicted example, server **104** is connected to network **102** along with storage unit **106**. In addition, 15 clients **108**, **110**, and **112** are connected to network **102**. These clients **108**, **110**, and **112** may be, for example, personal computers or network computers. In the depicted example, server **104** provides data, such as boot files, operating system images, and applications to clients **108**-  
20 **112**. Clients **108**, **110**, and **112** are clients to server **104**. Network data processing system **100** may include additional servers, clients, and other devices not shown.

In the depicted example, network data processing system **100** is the Internet with network **102** representing a 25 worldwide collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols to communicate with one another. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, 30 consisting of thousands of commercial, government,

Docket No. RSW920030303US1

educational and other computer systems that route data and messages. Of course, network data processing system 100 also may be implemented as a number of different types of networks, such as for example, an intranet, a local area 5 network (LAN), or a wide area network (WAN). **Figure 1** is intended as an example, and not as an architectural limitation for the present invention.

Referring to **Figure 2**, a block diagram of a data processing system that may be implemented as a server, 10 such as server 104 in **Figure 1**, is depicted in accordance with a preferred embodiment of the present invention. Data processing system 200 may be a symmetric multiprocessor (SMP) system including a plurality of processors 202 and 204 connected to system bus 206. 15 Alternatively, a single processor system may be employed. Also connected to system bus 206 is memory controller/cache 208, which provides an interface to local memory 209. I/O bus bridge 210 is connected to system bus 206 and provides an interface to I/O bus 212. Memory 20 20 controller/cache 208 and I/O bus bridge 210 may be integrated as depicted.

Peripheral component interconnect (PCI) bus bridge 214 connected to I/O bus 212 provides an interface to PCI local bus 216. A number of modems may be connected to PCI 25 local bus 216. Typical PCI bus implementations will support four PCI expansion slots or add-in connectors. Communication links to clients 108-112 in **Figure 1** may be provided through modem 218 and network adapter 220 connected to PCI local bus 216 through add-in boards.

Docket No. RSW920030303US1

Additional PCI bus bridges 222 and 224 provide interfaces for additional PCI local buses 226 and 228, from which additional modems or network adapters may be supported. In this manner, data processing system 200 5 allows connections to multiple network computers. A memory-mapped graphics adapter 230 and hard disk 232 may also be connected to I/O bus 212 as depicted, either directly or indirectly.

Those of ordinary skill in the art will appreciate 10 that the hardware depicted in **Figure 2** may vary. For example, other peripheral devices, such as optical disk drives and the like, also may be used in addition to or in place of the hardware depicted. The depicted example is not meant to imply architectural limitations with respect 15 to the present invention.

The data processing system depicted in **Figure 2** may be, for example, an IBM eServer pSeries system, a product of International Business Machines Corporation in Armonk, New York, running the Advanced Interactive Executive 20 (AIX) operating system or LINUX operating system.

With reference now to **Figure 3**, a block diagram illustrating a data processing system is depicted in which the present invention may be implemented. Data processing system 300 is an example of a client computer. Data 25 processing system 300 employs a peripheral component interconnect (PCI) local bus architecture. Although the depicted example employs a PCI bus, other bus architectures such as Accelerated Graphics Port (AGP) and Industry Standard Architecture (ISA) may be used. 30 Processor 302 and main memory 304 are connected to PCI

Docket No. RSW920030303US1

local bus 306 through PCI bridge 308. PCI bridge 308 also may include an integrated memory controller and cache memory for processor 302. Additional connections to PCI local bus 306 may be made through direct component

5 interconnection or through add-in boards. In the depicted example, local area network (LAN) adapter 310, SCSI host bus adapter 312, and expansion bus interface 314 are connected to PCI local bus 306 by direct component connection. In contrast, audio adapter 316, graphics

10 adapter 318, and audio/video adapter 319 are connected to PCI local bus 306 by add-in boards inserted into expansion slots. Expansion bus interface 314 provides a connection for a keyboard and mouse adapter 320, modem 322, and additional memory 324. Small computer system interface

15 (SCSI) host bus adapter 312 provides a connection for hard disk drive 326, tape drive 328, and CD-ROM drive 330.

An operating system runs on processor 302 and is used to coordinate and provide control of various components within data processing system 300 in **Figure 3**. The

20 operating system may be a commercially available operating system, such as Windows XP, which is available from Microsoft Corporation. An object oriented programming system such as Java may run in conjunction with the operating system and provide calls to the operating system

25 from Java programs or applications executing on data processing system 300. "Java" is a trademark of Sun Microsystems, Inc. Instructions for the operating system, the object-oriented operating system, and applications or programs are located on storage devices, such as hard disk

Docket No. RSW920030303US1

drive 326, and may be loaded into main memory 304 for execution by processor 302.

Those of ordinary skill in the art will appreciate that the hardware in **Figure 3** may vary depending on the 5 implementation. Other internal hardware or peripheral devices, such as flash read-only memory (ROM), equivalent nonvolatile memory, or optical disk drives and the like, may be used in addition to or in place of the hardware depicted in **Figure 3**. Also, the processes of the present 10 invention may be applied to a multiprocessor data processing system.

The depicted example in **Figure 3** and above-described examples are not meant to imply architectural limitations. For example, data processing system 300 15 also may be a notebook computer or hand held computer in addition to taking the form of a PDA. Data processing system 300 also may be a kiosk or a Web appliance.

The present invention provides an improved method, apparatus, and computer instructions for alternative 20 registry lookup of Web services without impacting existing client implementations. Instead of changing existing client implementation to accommodate changes of service endpoint location, an innovative registry lookup Java naming and directory (JNDI) provider is provided in 25 a client container for accessing Web services. The innovative registry lookup JNDI provider enables alternative registry lookup by leveraging the client programming model of the J2EE Web services (JSR-109).

Under the J2EE Web services client programming 30 model, a client may be a J2EE client application, a Web

Docket No. RSW920030303US1

component, an enterprise Java bean (EJB) component, or another Web service. A client may use the J2EE Web services run time environment to access and invoke methods of a Web service. In order to access a Web 5 service, the client uses a JNDI lookup to access a service object, which is then used by the client to retrieve a stub or proxy. A stub or proxy is the client representation of an instance of the Web service implementation. The JNDI lookup provides location of the 10 service endpoint to the client in the form of a URL.

In a preferred embodiment, the present invention provides an innovative registry lookup JNDI provider in a client container for looking up a service endpoint location in a registry. A registry, such as, for 15 example, a UDDI registry, includes concrete service locations published by the Web service provider. A registry may be implemented locally on the client, such as client 108 in **Figure 1**, or remotely on a server, such as server 104 in **Figure 1**, in the form of a registry 20 file.

When a service requester makes a request to lookup a Web service using JNDI, the innovative registry lookup JNDI provider in the client container looks up a service endpoint by first examining the service-ref-name element 25 of a new registry file, such as, for example, a UDDI registry file. Other types of registry file may also be used, such as, for example, a web service inspection language (WSIL) registry file, an electronic business using extensible markup language (ebXML) registry file or 30 a registry file that is implemented using a database.

Docket No. RSW920030303US1

The service-ref-name element represents the name value passed into the JNDI InitialContext object. The IntialContext object provides a starting point into the namespace from which the lookup is performed. The 5 service-ref-name element of the new registry file is examined to determine whether the service name requested is present in the file. An example requested service name is "service/TemperatureConverterService".

If the requested service name is present in the 10 service-ref-name element of the new registry file, the registry lookup JNDI provider uses information from other elements of the new registry file to retrieve a service endpoint location from the registry. Alternatively, if the requested service name is absent in the service-ref-15 name element of the new registry file, as determined by the alternative registry lookup JNDI provider, the alternative registry lookup JNDI provider defers the lookup operation and the service-ref-name element to a standard JNDI provider.

20 The standard JNDI provider then searches a webservicesclient.xml file for the corresponding service-ref-name element in order to identify the service endpoint location in an additional configuration file, such as, for example, a WSDL file. The 25 webservicesclient.xml file is a default deployment descriptor file defined in the J2EE Web services specification. The standard JNDI provider uses a wsdl-file element in the webservicesclient.xml file to identify the location of the WSDL file. Once the WSDL 30 file is located, the standard JNDI provider determines if

Docket No. RSW920030303US1

the service-ref-name element maps to the wsdl:service element of the WSDL file.

If a mapping occurs, the standard JNDI provider identifies the location of the service endpoint in the 5 wsdlsoap:address element of the WDSL file and returns the endpoint location to the service requester. However, if no mapping occurs, the standard JNDI provider may return an error to the service requester.

Thus, the mechanism of the present invention, an 10 innovative registry lookup JNDI provider, enables alternative registry lookup of the service endpoint URL of the invoked remote Web service, in place of the standard registry lookup through the wsdl:address element of the WSDL file. The alternative registry lookup may be 15 accomplished without the need of changing existing client implementation.

In addition, the alternative registry lookup JNDI provider may provide caching of the service endpoint 20 location obtained from the registry, which helps to avoid unnecessary lookups, hence, improves performance. The registry lookup JNDI provider may maintain a simple data structure, such as, for example, a hash map of local JNDI service names and service endpoint URLs that are retrieved previously. Prior to each registry lookup, the 25 registry lookup JNDI provider may examine the hash map to determine whether the requested service name had been looked up. If the requested service name had been looked up previously, the registry lookup JNDI provider returns the cache version of the service endpoint location from 30 the hash map, as opposed to performing a new lookup.

Docket No. RSW920030303US1

Furthermore, the alternative registry lookup JNDI may support multiple types of registries by allowing the client to specify an endpoint registry location, any required access control information for the registry, and 5 information required to locate the specific service and corresponding endpoint. Examples of other types of registry include UDDI registry, a web service inspection language (WSIL) registry, an electronic business using extensible markup language (ebXML) registry, and a custom 10 registry that is implemented using a database.

Turning now to **Figure 4A**, a diagram illustrating relationships between JNDI providers of the present invention is depicted in accordance with a preferred embodiment of the present invention. As depicted in 15 **Figure 4A**, JNDI provider **402** provides an abstract definition of the JNDI provider as defined in the JNDI specification. Examples of abstract definition required for the JNDI provider are context implementation, name parsers, URL context implementations, etc. However, 20 subclasses of the JNDI provider may implement a subset of the abstract definitions. With the present invention, there are two JNDI providers that implement JNDI provider **402**: J2EE JNDI provider **404** and registry lookup JNDI provider **406**. Registry lookup JNDI provider **406** 25 implements all of the abstract interfaces defined in the JNDI specification and delegates part of its implementation to another JNDI provider, in this example, J2EE JNDI provider **404**. In this way, if the requested service name is not present in the service-ref-name 30 element of the new registry file, registry lookup JNDI

Docket No. RSW920030303US1

provider 406 may delegate the lookup of service endpoint to J2EE JNDI provider 404. JNDI providers 404 and 406 may be implemented in a client container, which runs on a client, such as client 108 in **Figure 1**.

5       Turning now to **Figure 4B**, a diagram illustrating an example implementation of delegating lookup to a standard JNDI provider is depicted in accordance with the present invention. As depicted in **Figure 4B**, in this example implementation, registry lookup JNDI provider 440 includes a reference to standardProvider 442. When a service requester initiates a lookup 444 with service name 446 requested as the parameter. PrivateLookup 448 method, which is a method in registry lookup JNDI provider 440, performs lookup in the new registry file.

10      If the service name is found in the service-ref-name element of the new registry file, the stub of the endpoint URL found is returned. However, if no stub is returned as a result of privateLookup 448, registry lookup JDNI registry 400 defers the lookup operation to

15      standardProvider 442 by calling the lookup method 450 of standardProvider 442 and passing the service name 446 to lookup method 450 as an input parameter.

20      StandardProvider 448 performs the appropriate lookup in other registry files, such as, for example, a WSDL file

25      and returns the endpoint URL.

30      Turning next to **Figure 5**, a diagram of components used in the present invention is depicted in a preferred embodiment of the present invention. As depicted in **Figure 5**, client container 500 may be implemented as a client application that runs on a client, such as client

Docket No. RSW920030303US1

100 in **Figure 1**. A service requester or client directly interacts with client container 500 to request a Web service. When client container 500 receives the request, registry lookup JNDI provider 504 provided by the present 5 invention is used for alternative registry lookup.

Registry lookup JNDI provider 504 first examines a registry file, such as, for example, UddiLookup.xml file 505, for an element called service-ref-name.

If the service-ref-name element is present with the 10 requested service name, a lookup is performed by registry lookup JNDI provider 504 to retrieve the service endpoint URL from UddiLookup.xml file 505. Based on other information, such as a tModel name and a service key, in UddiLookup.xml file 505, the service endpoint URL may be 15 retrieved. From the retrieved service endpoint location URL, client container 500 may access service endpoint 514 by obtaining a stub implementation of port 512, which resides on Web container 510.

Alternatively, if no service-ref-name element is 20 present with the requested service name in UddiLookup.xml file 505, registry lookup JNDI provider 504 delegates the lookup operation to a standard JNDI provider, such as, J2EE JNDI provider 502, which then examines webservicesclient.xml file 508 to locate an additional 25 configuration file, in this example, WSDL file 506. WSDL file 506 includes a wsdl:address element that identifies the service endpoint URL. Similarly, based on this service endpoint URL retrieved by J2EE JNDI provider 502, client container 500 may access service endpoint 514, via

Docket No. RSW920030303US1

a stub implementation of port **512**, which resides on Web container **510**.

With reference to **Figure 6**, a diagram illustrating interaction between components used in the present invention is depicted in a preferred embodiment of the present invention. As depicted in **Figure 6**, service requester **600** may initiate a registry lookup request for a Web service by calling a lookup method of new registry lookup JNDI provider **602** and providing the requested service name as the parameter (call **620**). Upon receiving the request, registry lookup JNDI provider **602** examines the service-ref-name element of the UddiLookup.xml file **606** using the service name parameter and determines whether the service-ref-name element is present with the requested service name (call **622**). If the service-ref-name element is present with the requested service name, new registry lookup JNDI provider **602** examines UddiLookup.xml file **604** and identifies information, such as a tModel name and a service key (call **626**), necessary to retrieve location of service endpoint from UDDI registry **612**.

Alternatively, similar to the above example, upon initiation of lookup (call **630**) by service requester **600** and examining of service-ref-name element in the UddiLookup.xml file **606**, if the service-ref-name element is not present with the requested service name in UddiLookup.xml file **606**, new registry lookup JNDI provider **602** delegates the lookup and the service-ref-name element to a standard JNDI provider (call **632**), such as J2EE JNDI provider **604**. J2EE JNDI provider **604** then

Docket No. RSW920030303US1

searches webservicesclient.xml file 608 using the service-ref-name element for the location of WSDL file 610 (call 634). The location of WSDL file 610 is based on a wsdl:file element in webservicesclient.xml file 608.

5 Once WSDL file 610 is located, J2EE JNDI provider 604 determines whether the wsdl:service element in WSDL file 610 maps to the service-ref-name element of the webservicesclient.xml file 608 (call 636). If mapping occurs, J2EE JNDI provider 604 retrieves the service  
10 endpoint URL based on the wsdlsoap:address element of the WSDL file 610 (call 638).

With reference to **Figure 7**, a diagram illustrating an example client container implementation is depicted in accordance with a preferred embodiment of the present invention. As depicted in **Figure 7**, in this example implementation of client code 700, a service requester requests the initial context 702, which is a starting point into the namespace, to lookup 704 a service with a name of  
20 "java:comp/env/service/TemperatureConverterService". As a result of the lookup, a stub of TemperatureConverterService, TemperatureConverter 706, is retrieved based on the service endpoint URL provided by the new registry lookup JNDI provider. The stub acts as  
25 a proxy to the Web service requested, in this example, the TemperatureConverterService.

With reference now to **Figure 8**, a diagram illustrating an example implementation of the webservicesclient.xml file is depicted in accordance with 30 a preferred embodiment of the present invention. As

Docket No. RSW920030303US1

depicted in **Figure 8**, webserviceclient.xml file 800 includes service-ref-name element 802 and wsdl-file element 804. Service-ref-name element 802 declares a logical name that the client container uses to lookup a  
5 Web service.

When a standard JNDI provider is delegated to perform a lookup, the standard JNDI provider examines service-ref-name element 802 to determine whether it maps to the requested service name passed from the registry  
10 lookup JNDI provider. In this example, service-ref-name element 802 has a value of "service/TemperatureConverterService".

If a mapping occurs, the standard JNDI provider proceeds to examine wsdl-file element 808, which contains  
15 the URI location of a WSDL file. In this example, the location of the WSDL file is "WEB-INF/wsdl/TemperatureConverter.wsdl." The WSDL file is described in further details in **Figure 9**.

Turning now to **Figure 9**, a diagram illustrating an  
20 example implementation of a WSDL file is depicted in accordance of the present invention. As depicted in **Figure 9**, in this example implementation, WSDL file 900 is located by the standard JNDI provider using wsdl-file element 804 in **Figure 8**. WSDL file 900 includes  
25 wsdl:service element 902. When the standard JNDI provider examines wsdl:service element 902, a determination is made as to whether the name attribute maps to the requested service name in the service-ref-name element passed from the registry lookup JNDI  
30 provider. If a mapping occurs, the standard JNDI

Docket No. RSW920030303US1

provider looks up the location of service endpoint by examining the wsdlsoap:address element **904** of WSDL file **900**. In this example, the service endpoint is located at URL,

5 "http://localhost:9080/SOAPWithAttachments/services/TempC  
onverterService". From this URL, the standard JNDI provider may retrieve a stub of the service endpoint interface.

Turning next to **Figure 10**, a flowchart diagram  
10 illustrating an exemplary process of performing alternative registry lookup is depicted in accordance with a preferred embodiment of the present invention. As depicted in **Figure 10**, the process begins when a service requester initiates a lookup of a Web service by calling  
15 the lookup method of the initial context with a service name passed as a parameter (step **1000**). Next, the registry lookup JNDI provider examines the new registry file, such as UddiLookup.xml file, for a service-ref-name element (step **1002**). A determination is made as to  
20 whether the service-ref-name element is present in the new registry file (step **1004**). If the element is present, the registry lookup JNDI provider looks up the service endpoint location using information from the registry file (step **1010**). Once the service endpoint  
25 location is identified, the service endpoint location is returned to the service requester (step **1012**) and the process terminating thereafter.

Alternatively, if the registry lookup JNDI provider determines that the service-ref-name element is absent,  
30 the registry lookup JNDI provider defers the registry

Docket No. RSW920030303US1

lookup to a standard JNDI provider, such as, for example, a J2EE JNDI provider (step 1006) and the process terminating thereafter.

Turning next to **Figure 11**, a flowchart diagram illustrating an exemplary process of registry lookup performed by a standard JNDI provider is depicted in accordance with a preferred embodiment of the present invention. This flowchart provides a more detailed description of step 1006 in **Figure 10**. As depicted in 10 **Figure 11**, the process begins when a standard JNDI provider, such as, for example, a J2EE JNDI provider, locates the service-ref-name element in the default webservicesclient.xml file (step 1100). A determination is then made as to whether the service-ref-name element 15 of the webservicesclient.xml file maps to the service name passed from the service-ref-name element of the registry lookup JNDI provider (step 1102). If no mapping occurs, the standard JNDI provider returns an error to the service requester (step 1116) and the process terminating thereafter.

However, if mapping occurs in step 1110, the standard JNDI provider looks up the wsdl-file element in the webservicesclient.xml file (step 1104). The wsdl-file element from the webservicesclient.xml file is used 25 to identify location of the WSDL configuration file (step 1106). Once the WSDL file is located, the standard JNDI provider examines the WSDL file for a wsdl:service element (step 1108), which includes a name attribute. Next, a determination is made as to whether the service 30 name specified in the service-ref-name element delegated

Docket No. RSW920030303US1

by the registry lookup JNDI provider maps to the name attribute of the wsdl:service element (step 1110). If a mapping occurs, the standard JNDI provider looks up the wsdlsoap:address element of the WSDL file (step 1112),  
5 which includes location of the service endpoint. The standard JNDI provider then returns the service endpoint location in the wsdlsoap:address element to the service requester (step 1114) and the process terminating thereafter.

10 However, if no mapping occurs in step 1110, the standard JNDI provider returns an error to the service requester (step 1116) and the process terminating thereafter.

15 Turning now to **Figure 12**, a diagram illustrating an example implementation of a UDDI registry provider is depicted in accordance with a preferred embodiment of the present invention. As depicted in **Figure 12**, in order to obtain a lookup of a service endpoint URL for a JNDI local reference 1202, a UDDI service key and a tModel name is required. The UDDI service key and the tModel  
20 name are both located in a new registry file, in this example, UDDILookup.xml file 1206.

When a request is sent from a service requester, the registry lookup JNDI provider of the present invention  
25 obtains the service-ref-name from JNDI local reference 1202. Next, the provider examines UDDILookup.xml file 1206 and determines if corresponding service-ref-name element in UDDILookup.xml file 1206 is present. If corresponding service-ref-name element in UDDILookup.xml file 1206 is present, the registry lookup JNDI provider

Docket No. RSW920030303US1

uses the service-ref-name as a key to obtain the UDDI service key and the tModel name from the UDDILookup.xml file 1206, in order to retrieve the UDDI endpoint URL. The UDDI endpoint URL is then cached by the registry 5 lookup JNDI provider for future lookups.

However, if corresponding service-ref-name is not present in UDDILookup.xml file 1206, the registry lookup JNDI provider defers the lookup to a standard JNDI provider, which locates WSDL file 1208 via 10 webservicesclient.xml file 1204 and retrieves the endpoint URL from WSDL file 1208.

Turning now to **Figure 13**, a diagram illustrating an example implementation of the new UDDI registry file using a keyed policy is depicted in accordance with a 15 preferred embodiment of the present invention. As depicted in **Figure 13**, uddi-endpoint-lookup element 1300 is an example implementation of the new UDDI registry file, such as UDDILookup.xml file 1206 in **Figure 12**. In this example, uddi-endpoint-lookup element 1300 includes 20 a keyed-lookup-policy element 1302. Keyed-lookup-policy element 1302 includes a service-ref-name element 1304, which is examined by the registry lookup JNDI provider to determine if the requested service name is present. If service-ref-name element 1304 is present with the 25 requested service name, the registry lookup JNDI provider uses service-ref-name element 1304 as a key to obtain tModel-name 1306 and service-key element 1308. In this example, a keyed lookup policy is employed, which requires tModel-name 1306 and service-key element 1308 to

Docket No. RSW920030303US1

lookup an endpoint URL from UDDI-url 1310. The keyed lookup policy returns either zero or one endpoint URL.

In a case when the UDDI registry, in this example, uddi-endpoint-lookup element 1300, is searched using 5 other parameters, which return more than one endpoint URLs, a limiting algorithm may be used to determine the exact endpoint URL to choose by defining a lookup policy. An example of multiple endpoint URLs search may be a search of endpoint URLs that implements a particular 10 service provided by a particular company. With the present invention, the registry lookup JNDI provider may implement a number of lookup policies from the registry file, such as, for example, taking the first endpoint 15 from a list of endpoint URLs, or taking the endpoint URL that is available for the longest time.

Turning next to **Figure 14**, a diagram illustrating an example UDDI registry file using a lookup policy of the present invention is depicted in accordance with a preferred embodiment of the present invention. As 20 depicted in **Figure 14**, uddi-endpoint-lookup element 1402 is similar to uddi-endpoint-lookup element 1300 in **Figure 13**, except that a lookup policy is defined using business-lookup-policy element 1404. In this example, the search for an endpoint URL is according to business- 25 name 1406, IBM, and by service-name 1408, TemperatureConverter. Since multiple endpoint URLs may be returned from this search, a selection-policy 1410 is used to select only the first endpoint URL in the list, as specified by FIRST-IN-LIST.

Docket No. RSW920030303US1

During registry lookup, the registry lookup JNDI provider of the present invention can also handle lookup failures by directly reporting the error back to the service requester, or deferring the error to be handled 5 by the standard JNDI provider, which acts as a backup provider for obtaining a fixed endpoint URL. These error-handling functions may be performed using the NamingException mechanism, which is part of the JNDI specification.

10 Thus, the present invention provides an alternative registry lookup using an innovative registry lookup JNDI provider. The innovative registry lookup JNDI provider examines the service-ref-name element of the new registry file upon receiving a request for a Web service, and 15 determines whether the service-ref-name element corresponding to the requested service name is present in the new registry file. If the element is present, the registry lookup JNDI provider locates the service endpoint URL using information from the new registry 20 file. The registry lookup JNDI provider then retrieves the endpoint URL and returns it back to the service requester.

If the service-ref-element is absent in the new registry file, the registry lookup JNDI provider defers 25 the service-ref-name element with the requested service name to a standard JNDI provider, which then locates a WSDL file from a wsdl-file element in a webservicesclient.xml file. The standard JNDI provider then uses the deferred service-ref-name element as a key 30 to map to the wsdl:service element of the WSDL file. If

Docket No. RSW920030303US1

a mapping occurs, the standard JNDI provider retrieves the endpoint URL from the wsdlsoap:address element and returns it back to the service requester. If no mapping occurs, the standard JNDI provider instead returns an  
5 error back to the service requester indicating the failure.

In addition, the innovative registry lookup JNDI provider may improve performance of registry lookup by caching the endpoint URL retrieved for subsequent  
10 registry lookups using a data structure, such as, for example, a hash map. The registry lookup JNDI provider may also support other types of registries, such as, for example, a WSIL registry, a UDDI registry, an electronic business using extensible markup language (ebXML)  
15 registry, and a custom registry implemented using a database. This may be accomplished by allowing the client to specify the endpoint registry location and other necessary access control information in the registry lookup JNDI provider.

20 Furthermore, the innovative registry lookup JNDI provider may implement lookup policies in the new registry file. The lookup policies define specific rules governing selection of a particular endpoint URL in case of a lookup that returns multiple endpoint URLs. An  
25 error handling function may also be implemented in the registry lookup JNDI provider by using the NamingException mechanism to return lookup failures to the client or to defer error handling to another JNDI provider.

Docket No. RSW920030303US1

In summary, by using the innovative registry lookup JNDI provider, the need for changing existing client implementation is no longer required. The registry lookup JNDI provider also takes advantage of, rather than 5 in conflict with, the JNDI application programming interface (API) and the J2EE Web services specifications to provide an alternative mechanism for registry lookup of Web services. Finally, by caching the endpoint URLs retrieved previously, the registry lookup JNDI provider 10 eliminates the cumbersome task of performing a lookup each time a service is requested, thus, improves registry lookup performance.

It is important to note that while the present invention has been described in the context of a fully 15 functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention 20 applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media, such as a floppy disk, a hard disk drive, a RAM, CD-ROMs, DVD-ROMs, and 25 transmission-type media, such as digital and analog communications links, wired or wireless communications links using transmission forms, such as, for example, radio frequency and light wave transmissions. The computer readable media may take the form of coded

Docket No. RSW920030303US1

formats that are decoded for actual use in a particular data processing system.

The description of the present invention has been presented for purposes of illustration and description, 5 and is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in order to best explain the principles of the invention, 10 the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.